UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF OHIO
EASTERN DIVISION

JOHN DOE, ***on behalf of himself and all others similarly situated,***

Plaintiff,

v.

THE MISSION ESSENTIAL GROUP, LLC,

Defendant.

Case No. 2:23-cv-3365
Judge Sarah D. Morrison
Magistrate Judge Elizabeth Preston Deavers

OPINION AND ORDER

This matter is before the Court on the Motion to Dismiss (Mot., ECF No. 23) filed by The Mission Essential Group, LLC ("MEG"). Plaintiff John Doe[1] responded (Resp., ECF No. 24), and MEG filed a Reply (Reply, ECF No. 25). This matter is now ripe for consideration. For the reasons set forth below, Plaintiff lacks standing to assert his claims, and MEG's Motion is **GRANTED**.

I. FACTUAL BACKGROUND

The following summary draws from the allegations in the First Amended Class Action Complaint ("FAC"), as well as any documents integral to and incorporated therein.[2] (ECF No. 17 (public) / ECF No. 16 (sealed).)

[1] The Court previously granted Plaintiff leave to proceed under a pseudonym. (ECF No. 14.)

[2] "[W]hen a document is referred to in the pleadings and is integral to the claims, it may be considered without converting a motion to dismiss into one for

MEG is a private contractor that offers translation and interpretation services to the United States government, friendly foreign governments, and select private sector segments. (FAC, ¶¶ 1, 18.) MEG specializes in supporting "intelligence operations for warfighters" by providing "difficult-to-find language experts" in the Middle East, Africa, and Asia. (*Id.*, ¶ 19.)

Plaintiff was formerly employed by MEG as a translation expert. (FAC, ¶¶ 25, 44.) As a condition of his employment, Plaintiff provided MEG with certain personally identifiable information ("PII"), including, but not limited to, his full name and Social Security number. (*Id.*, ¶¶ 11, 26, 46.) MEG collects and maintains current and former employees' PII in its computer systems in accordance with federal and state law, industry standards, and its internal privacy policies. (*Id.*, ¶¶ 23, 27–28.)

In September 2022, federal law enforcement authorities alerted MEG "of a potential incident wherein certain [MEG] email accounts may have been accessed and/or acquired by an unauthorized actor." (FAC, ¶ 29; *id.*, Ex. A. ("Notice"), ECF No. 17-1, PAGEID # 183.) The types of PII that were "potentially present" in MEG email accounts included the full names and Social Security numbers of current and former employees and contractors and their spouses, dependents, or beneficiaries. (FAC, ¶ 29; Notice, PAGEID # 183.) Following an internal investigation, however,

---

summary judgment." *Doe v. Ohio State Univ.*, 219 F. Supp. 3d 645, 653 (S.D. Ohio 2016) (Graham, J.) (citations omitted); *see also Williams v. CitiMortgage, Inc.,* 498 Fed. App'x. 532, 536 (6th Cir. 2012) (per curiam) ("The law is clear that the Court may consider [a document] attached to the Complaint … in determining whether dismissal is proper.").

MEG "was unable to validate the reports from law enforcement" that any unauthorized access or data breach had occurred and was "unaware of any actual or attempted misuse" of PII. (FAC, ¶ 33; Notice, PAGEID # 183.)

"[O]ut of an abundance of caution," in July 2023, MEG notified Plaintiff and other current and former employees and contractors about the potential data breach (the "Data Incident"). (FAC, ¶ 35; Notice, PAGEID # 183.) The Notice did not convey when the Data Incident occurred, how MEG's network could have been hacked, or whether cybercriminals, terrorists, or hostile government actors were involved. (FAC, ¶¶ 5, 30.) In the Notice, MEG encouraged recipients whose PII may have been contained in an email account to "remain vigilant against incidents of identity theft and fraud" and offered one year of limited credit monitoring and identity restoration services. (*Id.*, ¶¶ 38, 40; Notice, PAGEID # 184–86.) MEG also confirmed that it was reviewing and updating its existing data protection and security policies and investigating additional security measures to ensure future protection of PII. (Notice, PAGEID # 184.)

Plaintiff believes that "one or more of [MEG's] employees gave malicious threat actors the credentials needed to access [MEG's] email accounts" through "basic social engineering techniques like phishing." (FAC, ¶¶ 31–32.) After receiving MEG's Notice, Plaintiff purchased anti-malware and anti-identity theft protection software on his and his family's electronic devices. (*Id.*, ¶ 52.) He also began receiving emails containing crypto-currency links, as well as "strange and concerning military-related emails" from unrecognized senders appearing to be of

Russian origin that promoted fraudulent offers for a military translation job. (*Id.*, ¶ 56.) Plaintiff believes these emails suggest that his PII "has been placed in the hands of cybercriminals, hostile government actors, and terrorists." (*Id.*)

II. PROCEDURAL HISTORY

Plaintiff commenced this putative class action against MEG in October 2023 and amended his Complaint shortly thereafter to add new claims and factual allegations. (ECF Nos. 1, 17.) In the FAC, Plaintiff alleges that due to MEG's failure to act with reasonable care and comply with standard security practices, an unknown actor was able to gain access to MEG's system via employee email addresses, thereby compromising and allowing third-party cybercriminals to acquire his sensitive PII and that of putative class members stored on MEG's network. (FAC, ¶¶ 1–4, 10, 23, 29.)

Plaintiff brings seven claims against MEG arising from the Data Incident:

- Negligence (Count I);
- Negligence *Per Se* (Count II);
- Breach of Implied Contract (Count III);
- Breach of Fiduciary Duty (Count IV);
- Invasion of Privacy / Intrusion upon Seclusion (Count V);
- Unjust Enrichment (Count VI); and
- Declaratory Judgment (Count VII).

(FAC, ¶¶ 96–163.)

As a result of MEG's failure to protect employees' PII and failure to sufficiently notify them of the Data Incident, Plaintiff alleges that he and the putative class have suffered or are at an increased risk of suffering various forms of harm, including: (1) lost time and effort monitoring accounts to prevent identity

theft; (2) costs associated with purchasing anti-theft protection software; (3) violation of privacy rights; (4) diminution in value of their PII; (5) increased risk of identity theft and physical danger; (6) an increase in "spam" or fraudulent emails; (7) the deprivation of the "earliest opportunity" to guard their PII due to a delay in notification of the Data Incident; and (8) emotional distress. (*Id.*, ¶¶ 48, 51–57, 63–70.) Plaintiff seeks damages and injunctive relief requiring MEG to employ adequate security practices consistent with law and industry standards to protect its users' PII. (*Id.*, ¶ 159, Prayer for Relief.)

MEG now moves to dismiss all claims against it. (Mot., PAGEID # 243.) MEG argues that Plaintiff lacks standing because his "sole basis for relief rests upon the risk of hypothetical harms" rather than a concrete injury-in-fact and because any alleged harm was caused by "independent actions of unknown third parties" and cannot be fairly traced to MEG. (*Id.*) Because this argument is dispositive, the Court need not address MEG's alternative arguments for dismissal.

III. STANDARD OF REVIEW

"Subject matter jurisdiction is a threshold matter that a court must decide prior to considering a claim's merits." *Boyd v. United States*, 932 F. Supp. 2d 830, 834 (S.D. Ohio 2013) (Marbley, J.). Without subject matter jurisdiction, a federal court lacks authority to hear a case. *Lightfoot v. Cendant Mortg. Corp.*, 580 U.S. 82, 92 (2017); *see also Kokkonen v. Guardian Life Insurance Co. of America*, 511 U.S. 375, 377 (1994) (federal courts are "courts of limited jurisdiction" that "possess only that power authorized by Constitution and statute"). Federal Rule of Civil

Procedure 12(b)(1) provides for dismissal when the Court lacks subject matter jurisdiction. "When subject matter jurisdiction is challenged under Rule 12(b)(1), the plaintiff has the burden of proving jurisdiction in order to survive the motion." *Madison–Hughes v. Shalala*, 80 F.3d 1121, 1130 (6th Cir. 1996).

Motions to dismiss for lack of subject matter jurisdiction fall into two general categories: facial attacks and factual attacks. *United States v. Ritchie*, 15 F.3d 592, 598 (6th Cir. 1994). Here, MEG puts forth a facial attack, which "questions merely the sufficiency of the pleading[,]" and the Court therefore takes the allegations of the FAC as true and construes them in the light most favorable to Plaintiff. (Mot., PAGEID # 247 n.4); *Wayside Church v. Van Buren Cty.*, 847 F.3d 812, 816 (6th Cir. 2017) (internal quotations omitted); *Ohio Nat. Life Ins. Co. v. United States*, 922 F.2d 320, 325 (6th Cir. 1990). To survive a facial attack, the complaint must contain a "short and plain statement of the grounds" for jurisdiction. *Rote v. Zel Custom Mfg. LLC*, 816 F.3d 383, 387 (6th Cir. 2016) (internal quotations and citations omitted). However, "conclusory allegations or legal conclusions masquerading as factual conclusions will not suffice to prevent a motion to dismiss." *Mezibov v. Allen*, 411 F.3d 712, 716 (6th Cir. 2005).

IV. ANALYSIS

Pursuant to Article III of the United States Constitution, standing is necessary to the exercise of jurisdiction and "determin[es] the power of the court to entertain the suit." *Warth v. Seldin*, 422 U.S. 490, 498 (1975); *see also TransUnion LLC v. Ramirez*, 594 U.S. 413, 417 (2021) (citation omitted) ("[U]nder Article III,

the plaintiff must have a 'personal stake' in the case—in other words, standing."). If the plaintiff lacks standing, then the federal court lacks jurisdiction. *Tennessee Gen. Assembly v. U.S. Dep't of State*, 931 F.3d 499, 507 (6th Cir. 2019).

To demonstrate Article III standing, the plaintiff must establish three elements:

> First, the plaintiff must have suffered an injury in fact—an invasion of a legally protected interest which is (a) concrete and particularized, and (b) actual or imminent, not conjectural or hypothetical. Second, there must be a causal connection between the injury and the conduct complained of—the injury has to be fairly traceable to the challenged action of the defendant, and not the result of the independent action of some third party not before the court. Third, it must be likely, as opposed to merely speculative, that the injury will be redressed by a favorable decision.

Lujan v. Defs. of Wildlife, 504 U.S. 555, 560–61 (1992) (cleaned up); *see also TransUnion,* 594 U.S. at 423 (citing *Lujan*). The plaintiff "bears the burden of establishing these elements" and must at the pleading stage "clearly ... allege facts demonstrating" each element. *Spokeo, Inc. v. Robins*, 578 U.S. 330, 338 (2016) (citations omitted); *Warth*, 422 U.S. at 338.

A. Injury-in-Fact

Injury is "the '[f]irst and foremost' of standing's three elements." *Spokeo*, 578 U.S. at 338–39 (quoting *Steel Co. v. Citizens for Better Env't*, 523 U.S. 83, 103 (1998)). "To establish injury in fact, a plaintiff must show that he or she suffered 'an invasion of a legally protected interest' that is 'concrete and particularized' and 'actual or imminent, not conjectural or hypothetical.'" *Id.* at 339 (quoting *Lujan*, 504 U.S. at 560). A plaintiff can demonstrate the existence of an injury-in-fact (1) by

showing that he suffered an actual injury as applied to him; (2) even if no actual injury in the traditional sense, by showing that the defendant violated a statute and thereby concretely harmed the plaintiff through the violation; or (3) by demonstrating an imminent risk of injury. *Foster v. Health Recovery Servs., Inc.*, 493 F. Supp. 3d 622, 631 (S.D. Ohio 2020) (Marbley, J.). Dismissal is proper only if all theories of injury-in-fact asserted under any of these three avenues are implausible. *Tate v. EyeMed Vision Care, LLC*, No. 1:21-cv-36, 2023 WL 6383467, at *8 (S.D. Ohio Sept. 29, 2023) (Cole, J.).

The federal circuits are split on what constitutes a sufficient Article III injury in data breach cases, which often involve allegations like those in this case of future or speculative fraud, identity theft, or other misappropriation of personal information. *See Kingen v. Warner Norcross + Judd LLP*, No. 1:22-CV-01126, 2023 WL 8544231, at *2 (W.D. Mich. Oct. 4, 2023). In the Sixth Circuit, *Galaria v. Nationwide Mut. Ins. Co.*, 663 Fed. App'x 384 (6th Cir. 2016), is instructive.[3] There, the plaintiffs sued their insurance company, alleging that hackers breached the company's network and stole their personal information; they sought damages for, among other things, the increased risk of fraud and the time and expenses they incurred in mitigating that risk. *Id.* at 385, 387. The Sixth Circuit concluded that the plaintiffs' allegations "of a substantial risk of harm, coupled with reasonably

[3] This Court has questioned *Galaria*'s viability after *TransUnion*, 594 U.S. 413, *see Brickman v. Maximus, Inc.*, No. 2:21-cv-3822, 2022 WL 16836186, at *3 (S.D. Ohio May 2, 2022) (Watson, J.), but the Sixth Circuit has yet to reconsider *Galaria* in light of *TransUnion*. Because this Court must follow relevant precedent from the Sixth Circuit, the Court applies *Galaria*.

incurred mitigation costs, are sufficient to establish a cognizable Article III injury at the pleading stage." *Id.* at 388. Because the *Galaria* plaintiffs claimed that "their data [was] stolen and [was] in the hands of ill-intentioned criminals," the court reasoned that the plaintiffs' alleged injury (the risk of future fraud) was "sufficiently concrete" because "a reasonable inference [could] be drawn that the hackers will use the victims' data for the fraudulent purposes alleged in [the plaintiffs'] complaints." *Id.*

With these principles in mind, the Court turns to the sufficiency of Plaintiff's alleged injuries in this case.[4]

1. Imminent Risk of Injury

Where plaintiffs seek to establish standing based on a risk of future harm that has yet to materialize, the "threatened injury must be *certainly impending* to constitute injury in fact," and "[a]llegations of *possible* future injury are not sufficient." *Clapper v. Amnesty Int'l USA*, 568 U.S. 398, 409 (2013) (internal quotations and citation omitted) (emphasis in original). Standing can be "based on a 'substantial risk' that the harm will occur," even where it is not "literally certain." *Id.* at 414 n.5 (citing cases); *see also Galaria*, 663 Fed. App'x at 388–89 (injury-in-

[4] The named plaintiff purporting to represent a class must have standing himself to seek relief on behalf of putative class members. *See Key v. DSW, Inc.*, 454 F. Supp. 2d 684, 687 (S.D. Ohio 2006) (Frost, J.) (quoting *Simon v. Eastern Ky. Welfare Rights Org.*, 426 U.S. 26, 40 n.20 (1976)) ("[A]ny named plaintiffs who represent a class 'must allege and show that they personally have been injured, not that injury has been suffered by other, unidentified members of the class to which they belong and which they purport to represent.'").

fact may be adequately pled based on "allegations of a substantial risk of harm, coupled with reasonably incurred mitigation costs").

Plaintiff alleges that he is at risk of future harm arising from (1) the potential for identity theft, fraud, or other scams; and (2) the potential for "physical harm" from unidentified entities and governments due to his position as a military translator. (FAC, ¶¶ 49, 65–68; Resp., PAGEID # 298–99.) However, he has not shown that these future risks are substantial or certainly impending.

Initially, and perhaps most problematically, Plaintiff has not sufficiently alleged that a data breach actually occurred. Plaintiff alleges that "[i]n September 2022, MEG … lost control over its computer network and the highly sensitive private information stored on the computer network in a data breach perpetrated by cybercriminals," such that Plaintiff and members of his proposed class "had their most sensitive personal information accessed, exfiltrated, and stolen." (FAC, ¶¶ 1, 4.) In support of this allegation, Plaintiff directs the Court to the Notice of Data Breach that he received from MEG. (*Id.*, ¶ 2 (citing Notice, PAGEID # 183).) But the Notice does not state that a data breach occurred—rather, the Notice states that MEG was "notified by federal law enforcement authorities of a potential incident wherein certain [MEG] email accounts may have been accessed and/or acquired by an unauthorized actor." (Notice, PAGEID # 183.) The Notice explains that "[a]fter a thorough and comprehensive investigation, [MEG] was unable to validate the reports from law enforcement and confirm unauthorized access to [MEG] email accounts occurred." (*Id.*) The Notice emphasizes that "there is no evidence of any

actual or attempted misuse" of information. (*Id.*) Although Plaintiff acknowledges this language (*see* FAC, ¶¶ 3, 29, 33), he offers no allegations of fact that contravene MEG's statements, only arguing in a conclusory fashion that the Notice was an ingenuine attempt by MEG to "downplay the severity" of the Data Incident. (FAC, ¶ 33.)

"[I]f a factual assertion in the pleadings is inconsistent with a document attached for support, the Court is to accept the facts as stated in the attached document." *Nat'l Ass'n of Minority Contractors, Dayton Chapter v. Martinez*, 248 F. Supp. 2d 679, 681 (S.D. Ohio 2002) (Rice, J.) (citing *The Mengel Co. v. Nashville Paper Prods. & Specialty Workers Union*, 221 F.2d 644, 647 (6th Cir. 1955)); *see also Williams*, 498 Fed. App'x at 536 ("[W]hen a written instrument contradicts allegations in the complaint to which it is attached, the exhibit trumps the allegations."). MEG's Notice states that it was unable to confirm or verify any unauthorized access or exfiltration of any data. "[T]he mere allegation of a risk of harm based on a data breach, without evidence of data theft or that the intruder accessed Plaintiff's specific information, is insufficient to state an 'imminent' injury for purposes of Article III standing." *Foster*, 493 F. Supp. 3d at 632. Without sufficient allegations of an actual data breach or unauthorized access, Plaintiff has not alleged a substantial risk of future harm. *See, e.g.*, *Sifuentes v. Pluto TV*, No. 1:23-CV-1013, 2023 WL 7319434, at *1 (W.D. Mich. Nov. 7, 2023) ("In *Galaria*, the plaintiffs alleged that their data had been stolen and was [ ] in the hands of ill-intentioned criminals … But Plaintiff makes no such allegation here. Instead, he

simply claims the existence of a breach of Defendant's firewall and from that speculates a parade of horribles."); *Williams-Diggins v. Mercy Health*, No. 3:16-CV-1938, 2018 WL 6387409, at *2 (N.D. Ohio Dec. 6, 2018) (emphasis in original) (finding lack of standing when plaintiff "only alleged that his personal information *might* be accessed improperly, not that it actually was"). Similarly, the Court doubts the imminency of any future harm to Plaintiff when nearly two years have passed since the alleged Data Incident with no signs that Plaintiff's PII has been accessed or misused. *See* Black's Law Dictionary (12th ed. 2024) (defining "imminent" to mean "threatening to occur immediately," "dangerously impending," or "about to take place").

Consequently, this case is distinguishable from *Galaria*. There, "hackers broke into [the defendant's] computer network and stole" plaintiffs' PII. *Galaria,* 663 Fed. App'x at 386. Thus, they "allege[d] that their data ha[d] already been stolen and [was] now in the hands of ill-intentioned criminals," and they "already knew that they [had] lost control of their data," meaning there was "no need for speculation" as to the substantial risk of harm. *Id.* at 388. Such is not the case here.

2. Actual Injury

Plaintiff also argues that he has sufficiently alleged concrete tangible and intangible harms as a result of the Data Incident, including (1) "reasonable mitigation costs" associated with purchasing anti-malware and anti-theft protection software for "all of his and his family's electronic devices"; (2) lost time and effort spent "verifying the legitimacy of the Notice … and self-monitoring his accounts and

credit reports"; (3) emotional distress; (4) his receipt of targeted scam or fraudulent emails; (5) the deprivation of the "earliest opportunity" to guard his PII due to MEG's delayed notification of the Data Incident; (6) violation of his privacy rights; and (7) property damage to his PII. (FAC, ¶¶ 48, 51–57, 63–70; Resp., PAGEID # 294–302.) The Court addresses each of these alleged injuries in turn.

Mitigation Costs. Looking first to the costs expended in purchasing protective software, in light of the fact that Plaintiff has not adequately alleged a substantial or impending risk of concrete harm, he did not "reasonably" incur these mitigation costs but rather acted based on his own speculative anticipation of harm. *See Clapper*, 568 U.S. at 416 ("Respondents' contention that they have standing because they incurred certain costs as a reasonable reaction to a risk of harm is unavailing—because the harm respondents seek to avoid is not certainly impending.").

Plaintiff argues that he "took these steps at MEG's direction," pointing to the Notice warning recipients to "remain vigilant against incidents or identity theft and fraud." (Notice, PAGEID # 184; Resp., PAGEID # 296.) But "remain[ing] vigilant" does not necessarily entail purchasing software for multiple devices, particularly when MEG had not identified a data breach but nevertheless offered a year of complimentary credit monitoring and identity restoration services. (FAC, ¶ 52; Notice, PAGEID # 184.) Plaintiff's mitigation expenses were made on his own volition "based on a nonparanoid fear" and do not qualify as actual injuries.

Lost Time and Effort. Plaintiff's next theory of injury fails because his allegations are, at best, conclusory as to his "efforts spent researching how to prevent, detect, contest, and recover from identity theft and fraud" and the "time spent verifying the legitimacy of the Notice of Data Breach, and self-monitoring his accounts and credit reports to ensure no fraudulent activity has occurred." (FAC, ¶¶ 50, 63.)

Further, even if Plaintiff had alleged these facts, his lost time and effort are not actual injuries for the same reasons as his purchase of protection software. Although it may have been reasonable to spend some time and effort to mitigate the risks associated with an actual data breach, these actions are not a concrete injury where there are no plausible allegations that Plaintiff's PII was accessed. If Plaintiff experienced lost time and effort, he did so trying to combat a speculative, potentially nonexistent threat.

Emotional Distress. Plaintiff asserts that he "has and is experiencing feelings of anxiety, sleep disruption, stress, fear, and frustration … far beyond allegations of mere worry or inconvenience." (FAC, ¶ 51.) Some courts find that emotional distress can be an injury-in-fact sufficient to confer standing—but only when there are allegations of actual unauthorized access or disclosure of data. *See, e.g.*, *Foster*, 493 F. Supp. 3d at 632; *McKenzie v. Allconnect, Inc.*, 369 F. Supp. 3d 810, 816 (E.D. Ky. 2019).

Targeted Fraudulent Emails. After the Data Incident, Plaintiff alleges that he received cryptocurrency links and "strange and concerning military-related

emails, including fraudulent offers for a military translation job, that appear to be of Russian origin … sent from unfamiliar Gmail addresses that Plaintiff does not recognize." (FAC, ¶ 56.) Despite the explicit conjecture in these allegations, the Court will consider the receipt of unsolicited commercial email communications to be a concrete harm, particularly in light of Plaintiff's sensitive geopolitical military background. *See Tate*, 2023 WL 6383467, at *5 (citing *Dickson v. Direct Energy, LP*, 69 F.4th 338, 345 (6th Cir. 2023), and observing that plaintiffs' receipt of "a significantly increased number of scam and phishing calls, texts, and emails" amounted to "a concrete and particularized injury—if barely").

Delayed Notice. Plaintiff argues that MEG's failure to discover and timely provide notification of the Data Incident made its employees "vulnerable" to "identity theft, without any warnings … to monitor their financial accounts and credit reports" and "imminent physical danger, without any warnings about how the Data Breach renders them sitting ducks for identification, capture and interrogation by terrorists and hostile government actors, particularly if they leave American soil." (FAC, ¶¶ 6, 7.) This speculative allegation is insufficient to establish an actual injury.

Violation of Privacy Rights. Plaintiff contends that his privacy rights were violated "when his private information was disclosed to cybercriminals" and "when cybercriminals disclosed his private information on the dark web—as evidenced by" his receipt of targeted scam emails. (FAC, ¶¶ 34, 53, 56; Resp., PAGEID # 302.) These allegations also fail because he has not alleged an actual disclosure or breach

occurred. Plaintiff's reliance on *Allen v. Wenco Mgmt., LLC*, 696 F. Supp. 3d 432, 437 (N.D. Ohio 2023), is unavailing—in *Allen*, the plaintiff alleged that he "received a data breach notification informing him that his personally identifiable information was accessed in the breach," and the defendant admitted that "an unauthorized person gained access to its network." ECF No. 1-1, *Allen v. Wenco Mgmt.*, No. 1:23-cv-103, ¶¶ 12, 29 (Jan. 18, 2023); *id.*, ECF No. 15, ¶¶ 12, 29 (Oct. 13, 2023).

Property Damage to PII. Finally, Plaintiff asserts diminution in the value of his PII because of the Data Incident and argues that "[c]ourts have held that a loss in value of personal information supports a finding that a plaintiff has suffered an injury in fact." (FAC, ¶¶ 54, 75; Resp., PAGEID # 301.) But, as discussed, he has failed to plead a data breach.

Moreover, Plaintiff does not allege that he ever tried to derive any value from his PII. *See, e.g.*, *Marlin v. Associated Materials, LLC*, No. 5:23CV1621, 2024 WL 2319115, at *3 (N.D. Ohio May 22, 2024); *Tate*, 2023 WL 6383467, at *12; *Lochridge v. Quality Temp. Servs., Inc.*, No. 22-CV-12086, 2023 WL 4303577, at *4 (E.D. Mich. June 30, 2023) ("Plaintiff does not allege any specific facts showing he planned to sell his information, just that it must have decreased in value because of the data breach … the court does not find that this suffices as an independent injury in fact sufficient to confer standing."). Plaintiff's contention that a "transfer of value" occurred because his PII "is likely already available on the dark web" is an assumption that does not equate to injury. (FAC, ¶ 75.)

C. Traceability

Because Plaintiff has sufficiently alleged an injury-in-fact for his receipt of allegedly targeted scam emails, the Court looks to whether he has adequately proven traceability. *Lujan*, 504 U.S. at 560–61; *Spokeo*, 578 U.S. at 338.

To establish standing, a plaintiff must demonstrate a "causal connection between the injury and the conduct complained of—the injury has to be fairly traceable to the challenged action of the defendant, and not the result of the independent action of some third party not before the court." *Lujan*, 504 U.S. at 560 (internal quotations and citations omitted). The plaintiff "must plausibly tie the claimed harm to the challenged conduct." *Tate*, 2023 WL 6383467, at *6. A defendant is not liable for injuries that are too remote, purely contingent, or indirect. *Holmes v. Sec. Inv. Prot. Corp.*, 503 U.S. 258, 268 (1992). "The standard for establishing traceability for standing purposes is less demanding than the standard for proving tort causation." *Buchholz v. Tanick*, 946 F.3d 855, 866 (6th Cir. 2020).

Here, Plaintiff has not demonstrated that the fraudulent emails he received are fairly traceable to the Data Incident or MEG's actions. Among other failures, he does not allege that his email address was accessed during the Data Incident. Although he insists that the PII possibly accessed in the Data Incident (including his name and Social Security number) can be "combined" with other sources to create "Fullz" packages that can be sold or used to commit fraud (FAC, ¶¶ 65–67), this chain of events relies not only upon the assumption that PII in MEG's

possession was improperly accessed, but also upon speculation about the actions of independent actors in combining the PII with information obtained elsewhere.

Additionally, various other actors could have sent Plaintiff the at-issue emails, including non-malicious commercial entities like recruiters seeking applicants for military-related jobs. His hypothetical and conclusory contentions of menacing connections between the emails and their senders will not suffice to prove traceability. *See Mezibov*, 411 F.3d at 716.

D. Redressability

Because Plaintiff has not demonstrated an injury-in-fact that is traceable to MEG or the Data Incident, the Court need not evaluate redressability.

V. CONCLUSION

Plaintiff is correct that "a plaintiff whose Social Security number is stolen in a data breach suffers concrete injury for the purpose of Article III standing." (Resp., PAGEID # 294 (citing *Galaria*, 663 Fed. App'x at 387–90).) However, he has not adequately pleaded that any of his PII was improperly accessed, let alone stolen. For this reason, and the reasons set forth above, MEG's Motion to Dismiss is **GRANTED**.